1969

Computers and Federal Regulation

John D. Leshy
UC Hastings College of the Law, leshyj@uchastings.edu

Calvin Davison

Stephen L. Babcock

Author: John D. Leshy

Source: Administrative Law Review

Citation: 21 Admin. L. Rev. 287 (1969).

Title: *Computers and Federal Regulation*

This is the first of what the Review hopes will be a series of contributions on the computer and Federal regulation. As a manuscript it covers a broad spectrum ranging from developments in Congress, before the Federal Communications Commission, as well as copyright, patent, antitrust, and export control problems.—The Editors

COMPUTERS AND FEDERAL REGULATION

BY CALVIN DAVISON*, STEPHEN L. BABCOCK**, JOHN D. LESHY***

Throughout our complex industrial society in the laboratory, in the factory, in transportation enterprises and elsewhere—the use of the computer has been a fact of life for many years. The federal government, of course, with its immense bureaucracy and masses of data to manipulate, evaluate, store and retrieve is a large and growing user of computers. Since the technological fact, however, often precedes an awareness of its total impact on society, the federal government in its governmental and regulatory capacity only now is beginning to consider the social and economic role of the computer and whether, or to what extent, legislation or other regulation is necessary or desirable in this field.

The purpose of this article is to survey the development to date of the federal government's concern with the field of computers. Based on this knowledge, it is possible to foresee to a certain extent the direction that the federal government's involvement in this area will take in the future. Also, knowledge of past developments will assist those interested in computer science in shaping the course of governmental participation to best meet the needs of the public and private interests involved. While predictions are always hazardous, it seems probable that involvement of the federal government will be greater than in the past for, aside from all other considerations, a principle that has been enunciated recently seems to be well grounded in fact:

> In analyzing government for a similar principle (to that of the profit motive in business), we are led to the conclusion that government officials generally seek to maximize the power of their positions.[1]

---

*Calvin Davison, member of the bar, District of Columbia. Miami University (A.B.). Harvard University (LL. B.). Partner, Reavis, Pogue, Neal & Rose, Washington, D.C.

**Stephen L. Babcock, member of the bar, District of Columbia. College of William & Mary (A.B.). University of Chicago (J.D.) Associate, Reavis, Pogue, Neal & Rose, Washington, D.C.

***John D. Leshy, Harvard College (A.B.); third year student Harvard Law School.

[1]Speech by Honorable Lee Loevinger, Commissioner, Federal Communications Commission, at The International Conference on Communications of The Institute of Electrical and Electronic Engineers, Philadelphia, Pennsylvania, June 13, 1968.

Since the computer is simply a sophisticated tool for the achievement of a variety of ends, it is manifest that almost all agencies and arms of the federal government will have some involvement with its development as that development affects the particular field of their concern. This article, therefore, will restrict its scope to only those areas of pronounced governmental concern or areas peculiar to the computer itself and not simply to its use as a tool to achieve other ends. Thus, particular attention is given to developments in Congress, before the Federal Communications Commission, in the copyright and patent field, in the antitrust field and in the area of export controls.

Regulatory Concerns of the Federal Communications Commission

The most active arena of federal regulatory concern in the computer field is presently before the Federal Communications Commission. In its inquiry into the interrelationship of computers and communications,[2] the FCC has squarely before it a whole parcel of issues involving the future of government regulation of computer services.

In addition several other proceedings before the FCC have had or will have a direct effect on computer activites. For example, in the *Carterfone Case* the FCC has decided that AT&T's long-established tariff rule prohibiting for all intents and purposes the attachment of non-AT&T devices to communications lines furnished by AT&T must be eliminated and be replaced by technical standards for attaching such so-called "foreign devices". This decision, of course, is of vital interest to all equipment manufacturers and to users, as well, who wish to attach their own equipment, including computers, to lines leased from communications common carriers. In its Sicom and Info-com decisions regarding services rendered by Western Union, the FCC has laid down certain guidelines for the future participation of communications common carriers as computer utilities. In addition, these decisions are of great interest to others who furnish computer services.

Of less direct interest, but nevertheless of great importance to the computer field, are other recent and pending proceedings before the FCC involving communications rates and practices. These are of vital concern to the "real time" use of computers since connection to communications lines is of vital importance for such use. In the satellite communications field, the FCC has determined in the *Authorized User Inquiry*, Docket No. 16058, that normally only communications common carriers may deal directly with COMSAT in the international field.[3] Thus, internationally, COMSAT will be mainly a

[2]Docket 16979.

[3]Mem. Opinion & Order FCC 66-677, 4 F.C.C.2d 421 (1966).

carrier's carrier. Other entities may deal directly with COMSAT only in unique circumstances where their needs cannot be met through the existing communications common carriers. One rationale for this decision is to preserve a balanced communications system internationally, rather than allow satellite technology to take advantage of its natural technical and economic superiority. In the pending *Domestic Satellite Inquiry*, Docket No. 16495 the FCC is investigating who should be allowed to operate domestic satellite systems—COMSAT, existing communications common carriers, or both—and whether other enterprises such as television networks should be allowed to operate private domestic satellite systems.

Finally, the rates for communications services, particularly for bulk users, are under exploration and severe attack in multiple FCC cases. Among these are Docket 16258, an investigation of the proper rate making principles to apply to AT&T's different classes of services and the relationship of those different classes of service; Docket 17457, an investigation of who, if anyone, should be allowed to share in the purchase of AT&T's bulk rate offering called Telpak; and Docket 18128, an investigation of the specific rates for AT&T's private line offerings. In addition, such cases as the *MCI Case*, Docket 16509, present to the Commission questions on whether specialized communications services will be allowed to be offered to the public by others than the existing communications common carriers.

The widest in scope of the various formal proceedings currently before the Federal Communications Commission is the *Computer Inquiry*, Docket No. 16979, formally entitled "Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities." In its *Notice of Inquiry* dated November 9, 1966,[4] initiating that investigation, the Commission stated that "effective use of the computer is . . . becoming increasingly dependent upon communication common carrier facilities and services by which the computers and the user are given instantaneous access to each other."[5] In amplification of this assertion, the Commission noted that most of the computers utilized by the varieties of firms offering data processing and information services can be programmed to provide message and circuit switching services in addition to their basic data processing and retrieval duties.

Further, the communications common carriers, presently beginning

---

[4] FCC Order 66-1004.
[5] *Id.* at par. 1.

to use computers as replacements for electro-mechanical switching machines, have a strong incentive to offer information and data processing services in order to minimize the costs associated with the operation of their computer equipment. Some common carriers, the Commission added, had already announced plans to provide specialized and general information services on a large scale. The result of this convergence of communications and information science technology, the Commission noted, is that both communications common carriers and members of various segments of the unregulated computer industry are, or soon will be, offering combined computer-communication services, and therefore, the Commission concluded "we are confronted with determining under which circumstances data processing, computer information and message switching services, or any particular combination thereof - whether engaged in by established common carriers or other entities - are or should be subject to the provisions of the Communications Act."[6]

The definition of "communication by wire" contained in section 3(a) of the Communications Act of 1934, 49 U.S.C. § 153(a), upon which the Commission's jurisdiction is based, was held in 1944 to include a customer's private terminal equipment (a hotel telephone exchange and the extensions attached thereto),[7] when connected to communications facilities offered by regulated communications common carriers, and this case can be construed as supporting the proposition that the Federal Communications Commission's jurisdiction extends over any device or system which is connected to the public telephone facilities of the communications common carriers subject to its regulation. On the other hand, it is obviously unlikely that the Commission would ever assert, much less attempt to exercise, a supposed right to control the use of such things as stamping and rolling mill equipment used in the production of steel, even though it were shown that such machinery was electrically connected to control computers which were in turn connected to communication facilities furnished by communications common carriers.

This jurisdictional aspect of the *Computer Inquiry*, which carries with it implications both concerning the types of computer services which unregulated entities will be able to offer, and, as well, the extent to which the existing common carriers will be allowed to enter the field,

---

[6] *Id.* at par. 18.

[7] *United States* v. *American Telephone & Telegraph Co.*, 57 F. Supp. 451 (S.D.N.Y. 1944); *Cf.*, *Ambassador, Inc.* v. *United States*, 325 U.S. 317 (1945).

is the focus of most of the interest of the parties who have responded to the Notice of Inquiry.

The *Computer Inquiry* also, however, is concerned with two additional subjects. The first group of these issues involves the rate levels and conditions of service established by the communications common carriers in connection with facilities to be used for the transmission of data. In its Notice of Inquiry the Commission indicated its interest in receiving views of the public on such matters as the right of communications common carriers customers to allow others to use their facilities, whether special rate levels should be established for communications facilities used for data transmission, whether customers should have the right to use their own terminal equipment, including multiplexing equipment to derive a large number of channels from a single channel leased from the communications common carrier, and whether the communications common carriers should be required to provide channels with special characteristics suitable for data, as opposed to voice, transmission. This group of issues, which can be characterized as related to the kinds of computer related communication services which should be provided, rather than with the question of what types of firms should provide composite data processing-communications services, may well prove to be of major importance to the general public in the years to come.

The other major group of issues included within the *Computer Inquiry* is the emotionally charged subject of the privacy of data stored in computers connected to communications lines. This subject, as noted in a subsequent section of this article, has already generated Congressional concern. The necessity for procedures adequate to protect personal information from unauthorized disclosure is especially apparent in the case of computers connected to communications lines and hence potentially accessible through the public telephone network. These considerations led the Commission to ask members of the computer and communication industries to delineate currently enforced protective measures and to make recommendations as to legislative or other action felt necessary to increase the existing standards of protection or to preserve them from deterioration.

Because the *Computer Inquiry* deals with subjects whose ramifications are unusually complex, and perhaps because of the fact that literally thousands of pages of material were submitted in response to the Commission's request for information, the Commission awarded a contract to Stanford Research Institute, a well-known California consulting organization, to examine the responses in light of the issues

involved and to submit detailed recommendations to the Commission for its review. After this report (currently expected in the spring of 1969) is received, the Commission may provide further opportunity for comments by interested parties and/or set selected issues for oral hearing. Thus the *Computer Inquiry* will not be finally resolved for some time in the future.

While this general investigation may be pending for some time to come, many of the issues included within its scope have been the subject of adjudicatory matters involving more precise and narrower questions. One of the most important of these is the well-known *Carterfone Case*.[8] The Carterfone is a device which acoustically and inductively connects mobile radio systems to the public telephone network. Connection is accomplished by placing a standard telephone hand set on a cradle which is furnished as a part of the Carterfone. Over a number of years, the Carterfone's manufacturer encountered continual opposition by communications common carriers to the use of the device, in the form of threats to disconnect telephone service furnished to those who used the Carterfone. Carter Electronics Corporation brought an action for treble damages under the antitrust laws against the telephone companies. The Court referred the matter to the Commission, however, invoking the doctrine of primary jurisdiction,[9] and the Commission thereupon instituted an investigation to determine whether the tariff provisions which prohibited the use of the Carterfone device in connection with message toll service were unjust, unreasonable or discriminatory in violation of the Communications Act. Carter thereafter filed a formal complaint against the communications common carriers involved, and this action was consolidated for hearing and decision with the Commission's own inquiry.

The Commission ultimately concluded that the provisions of AT&T's Tariff FCC No. 263 which prohibited "foreign attachments" and "interconnection" were unreasonable and should be stricken:

> "A customer desiring to use an inter-connecting device to improve the utility to him of both the telephone system and a private radio system should be able to do so, so long as the inter-connection

---

[8]Use of the Carterfone Device in Message Toll Telephone Service, Docket No. 16942, and *Carter Electronics Corp.* v. *American Telphone & Telegraph Co., et al*, Docket No. 17073. AT&T has decided not to appeal this decision.

[9]*Carter* v. *American Telephone & Telegraph Co.*, 250 F.Supp. 188 (N.D. Tex. 1966) *aff'd.*, 365 F.2d 486 (5th Cir. 1966).

does not adversely affect the telephone company's operations or the telephone system's utility for others. A tariff which prevents this is unreasonable."[10]

The commission thus eliminated the tariff provisions prohibiting foreign attachments and inter-connections with a statement whose implications are extremely broad. The eventual effect of the decision, however, remains unclear. The American Telephone & Telegraph Company's immediate response was to transmit, on September 13, 1968, revisions to its Tariff FCC No. 263 which would allow the use of customer-provided terminal equipment in connection with its toll message service, and which would allow the inter-connection of mobile radio systems. Then, On October 21, 1968, and November 11, 1968, AT&T filed additional tariff proposals, which became effective on January 1, 1969, and allow the inter-connection of any type of private communications system, such as a microwave system of the type used by large public utilities or an intra-office local telephone system, to the message toll service (now called message telecommunications service) furnished by the telephone company. In letters transmitting these filings, AT&T also announced that it would soon file revisions to its Private Line Service Tariff, FCC No. 260, which will permit the inter-connection of private communication systems, and the use of customer-provided terminal equipment, with Telpak and other inter-exchange channels leased from AT&T. The Commission, while permitting the filed revisions to become effective, laid plans for a series of informal discussions in the spring of 1969, on such questions as whether Bell should be ordered to permit customers to use their own devices to generate dialing, or "network control" signals. While the standards for customer-provided terminal equipment may be further revised to satisfy the objections of some user parties, and while many other similar subsidiary matters remain to be determined, it is thus now clear that telephone users will in the future be able to connect a wide variety of devices and systems to the public telephone network.

A second matter involving one of the issues in the *Computer Inquiry* is the Commission's decision concerning Western Union's Sicom and Infocom services.[11] Sicom service was proposed by Western Union in a tariff filed on September 22, 1967, in which Western Union proposed

---

[10] *Carterfone Case*, 13 FCC 2d 240, 424 (1968) (reconsideration denied, 14 FCC 2d 571) (September 11, 1968).

[11] *Western Union Telegraph Co., Tariff FCC No. 251*, 11 FCC 2d 1 (1967); *Western Union Telegraph Co., Tariff FCC No. 252*, 11 FCC 2d 15 (1967). (Info-com is a service similar to Sicom, but not specifically designed for brokerage firms.)

to provide to subscribing brokerage houses "store and forward" services for communications between the various offices of each customer. All messages would be forwarded to a computer provided by Western Union, which would forward them to their destination according to their priority, and adjust certain records which would remain available to the customer.

Under the tariff filing, a customer pays an "access line charge" for equipment located on his premises and the line connecting the customer's equipment to a shared 2300-baud data channel terminating in selected major cities located throughout the country, a "network charge" for the use of the shared data channels leading to Western Union's switching computer, and a "useage charge" depending upon the number of characters transmitted and received by the customer.

Over the objections of the Bunker-Ramo Corporation and others engaged in supplying similar services using lines leased from the communications common carriers, the Commission decided that the services Western Union would provide would not include "any significant non-common carrier, non-communications services . . . ."[12] The Commission conceded that the Sicom service might include some services, such as the performance of error checks, the implementation of transmission priorities, and the storage and retrieval capability, which might not be considered communication services when viewed alone. The Commission concluded, however, that "it is clear that a principal function of the computers in the Sicom service will be message switching, which is an integral function of a communication service."[13] The tariff, therefore, considered as a whole, did not warrant rejection or suspension on the ground that a non-communication service was being offered. The Commission added that its determination, however, would not prejudice any possible course of action which might be warranted in the light of the pending *Computer Inquiry*.

This differentiation between message switching and circuit switching nas also received attention in more recent Commission orders[14] concerning tariff provisions filed by Western Union International, Inc., on May

[12] 11 FCC 2d at 8.
[13] *Id.* at 9.
[14] FCC Order 68-1057, dated October 23, 1968.

29, 1968, to provide Deferred Overseas Datel Service.[15] In the initial order, the Commission set an investigation of the tariff. When the carrier withdrew its filing, however, the Commission terminated the proceeding without disposing of the questions raised in its initial order.

Datel service is a dial-up, high-speed data transmission service similar to the domestic services offered by the Western Union Telegraph Company and American Telephone & Telegraph Company, using voice-grade channels. In the Deferred Datel offering, Western Union International had proposed, for a five dollar additional charge, to store a message transmitted from the originating office and to re-transmit it to its destination at a later time specified by the customer. In its order instituting the investigation, the Commission stated that existing common carrier services should be considered as being divided into two categories; message services and customer-to-customer services. The first class of service includes an undertaking by the carrier to transmit a particular message over its facilities, and includes compensation both for the use of the transmission facilities and for the handling of the message transmitted. The second category, however, involves only an undertaking "to furnish a communication path connecting the customer with his correspondent . . . ."[16] The proposed Deferred Datel, however, would have involved both functions, and the Commission concluded that "new principles must be formulated to govern the charges, terms, and conditions upon which such a hybrid service is to be offered."[17]

While the investigation has been terminated, the opinion accompanying the order of investigation is of importance to those in the computer field because of its careful analysis of the differences between the furnishing of circuits and the handling of messages transmitted over those circuits, which in turn is related to the distinction between "communication services" and "non-communication services" referred to earlier.

It is apparent the three foregoing Commission cases are themselves related to the *Computer Inquiry*, in the same sense that computers themselves have become "inextricably intertwined" with communications. One of the obvious issues resulting from the *Carterfone* decision, for example, is that if customers may either lease terminal equipment from Bell or purchase it from independent sellers, the same opportunity for discrimination on the part of the common carriers exists as in the situation in which both regulated and non-

[15] Western Union International, Inc., Tariff FCC No. 11, Docket No. 18363.

[16] *Id.* at Par. 3.

[17] *Id.* at Par. 4.

regulated entities are competing in the offering of computer services in connection with communication facilities leased from the common carriers. Likewise, if the Commission's somewhat off-hand conclusion in the *Sicom* case, that message switching is an "integral function of a communication service" remains unmodified, entities which are not communications common carriers may eventually be denied the right to provide computer services in which "message switching" predominates.

Another recent development, which is not at the present time the subject of a hearing, is AT&T's new private line shared use regulations. By revisions which became effective on February 1, 1969, the Bell System has allowed its customers, in return for a 10% additional channel charge, to share the use of private lines (excepting full-time and alternate-use foreign exchange lines) purchased on an individual basis. This offering may well prove to be of great value to users of remote computer input-output devices, for it will allow such users to share the cost of interstate access lines with other users located in the same city.

Apart from those cases dealing specifically with computers and computer-related tariff offerings, several investigations before the Commission concern matters which will vitally affect the status of the various computer industries in the years to come. The *AT&T General Rate Investigation*, Docket No. 16258, includes an examination into rate-making principles for various classifications of American Telephone & Telegraph Company's communications services. If, as AT&T advocates, the Commission allows it to adopt "full additional cost" principles for services which are characterized by high elasticities of demand, AT&T might in the future find it to its advantage to offer lower rates for data transmission traffic, in cases in which the traffic otherwise would not move at all. It is probable that much computer-generated communications traffic is highly elastic, in the sense that the computer-using entity may be faced with a choice between a central computer with many radiating communications lines, on the one hand, and, on the other hand, the use of a larger number of smaller computers or the use of non-computerized mechanical data processing methods. Further, much of this traffic could move in off-peak nighttime hours. Thus, while the principal justification for using full additional costing principles is, presently, the threat of private microwave communication systems, regulatory approval of added cost ratemaking principles could benefit computer users substantially. The final resolution of this question of rate-making principles, however, may be made only in the latter part of 1969 or in 1970.

The historic pricing policies of regulated communications common carriers are under examination in other pending Commission cases. In

the *Telpak Sharing Investigation*, Docket No. 17457, the witness sponsored by the Common Carrier Bureau of the Federal Communications Commission has alleged both that the existing Telpak sharing provisions[18] unlawfully discriminate against those firms not entitled to share, and that the Telpak offering itself is unlawfully discriminatory in favor of large users as opposed to those who require only one or a few leased communication channels. While the latter proposition is, arguably, outside the scope of the *Telpak Sharing Investigation* itself, these views could eventually lead to a restructuring of AT&T's entire bulk communications offerings. The hearing in the *Telpak Sharing Investigation* terminated in September of 1968, and this case will probably be determined by the Commission in 1969. Another historic pricing principle, that of pricing both message telecommunications and private line services on a per-mile rate determined by averaging the costs for providing service in all markets throughout the United States, may be affected by the outcome of an additional pending case.

In the application of *Microwave Communications, Inc.*, FCC Docket 16509, *et al.*, an examiner has recommended authorizing a microwave communications common carrier to provide inter-plant and other similar leased line services between Chicago, Illinois, and St. Louis, Missouri, via nine intermediate cities. The applicant proposed rates of approximately half those charged by the existing communications common carriers for circuits of similar size, and the existing common carriers argued that to allow competition on the lower-cost "thick" inter-city markets would require them to raise their rates for services to smaller cities, over routes traversing unfavorable terrain, and in other situations in which the cost of providing service is higher than average for the entire nation. At least at the present, computer users are in general concentrated in the larger cities in the United States. Therefore, the abandonment of nation-wide averaging would lower their communication rates. The prospect of rate cases involving the examination of the costs of providing service over each and every communications route in the country, however, staggers the imagination. On the other hand, the cross-subsidy involved in situations in which some users (those located in isolated areas) are subsidized by users located in areas in which communication facilities actually are cheaper to provide, is, at the very least, less than rational from an economic point of view. The initial decision in this case was released on

[18]These allow public utilities and other entitites whose rates are regulated and state and federal government agencies to share the use of AT&T's bulk channel offering.

October 17, 1967, and a decision by the Commission is expected at any time.

Patent and Copyright Protection For Computer Programs

The area of computer technology and federal regulation that has provoked the most comment and debate has been the protection of the computer program. This in itself illustrates the crucial nature of the program in the computer process. The program is simply a code of step-by-step instructions that guides the computer through to the solution of whatever problem has been posed. Without a program, the computer is a hopeless idiot. Indeed, the advantage that is taken of the computer's enormous capabilities is largely dependent on the skill of the programmer. The computer must be programmed to perform every single logical step in reaching a conclusion. Every term and operation must be made explicit, and not one scintilla of thought process can be presumed, implied, or based on intuition. "In other words, the computers can do anything we tell them to do; their only absolute limitation is our ability to provide instructions."[19]

The present state of the law is that copyright protection is available to computer programs while patent protection is more debatable. The Copyright Office announced in 1964 that it would "consider" the registration of computer programs if the following factors were present: (1) original authorship, (2) publication, and (3) copies.[20] On May 8, 1964, the Copyright Office issued the first copyright for a program.[21] The position of the Copyright Office was based on the general language of the present Copyright Act, 17 U.S.C. 1 *et ff.*, and the Office freely conceded that it was a debatable question whether the programs were legally copyrightable. This protection apparently has not been especially attractive to program producers, however, because only fifty-two programs had been copyrighted by June 1966,[22] in spite of the fact that the procedure for obtaining such protection is quite simple. The protection for the form of the expression is secured ". . . by publication thereof with notice of copyright required by this title . . ."[23]

The Patent Office has not been so receptive to the idea of offering protection to computer programs. The statutory requirement for patentability is that there be a "new and useful process, machine,

[19]Loevinger, "The Methodology of Legal Inquiry," *Symposium, Jurimetrics, in 28 Law and Contemporary Problems* 1, Winter 1963, p. 32.

[20]Copyright Office, *Announcement*, 11 Bull. Copyright Soc'y 361 (1964).

[21]*New York Times*, May 8, 1964, p. 43, Cols. 4-6.

[22]Titus, "Copyrighting Computer Programs," 9 Communications ACM 879 (1966).

[23]17 U.S.C. 10.

manufacture or composition of matter."[24] The "process" aspect has been considered most fruitful by proponents of patentability. There is also the requirement that the subject matter to be patented must be an innovation, and not apparent to a person "having ordinary skill in the art."[25] It is doubtful whether many computer programs would be considered innovative under this test. The Patent Office in 1966 released a set of "Guidelines to the Examination of Programs".[26] These guidelines were defined as "a tenative theoretical analysis of applicable statutory law." Although they did not flatly reject the notion of patentability, they interpreted the law as to almost surely preclude any possibilities of widespread patentability of computer programs. In October 1968 the Patent Office issued a guideline which stated that it was not going to grant patents for programs unless they were embodied in a mechanical device. The patent laws offer a much broader protection than the copyright laws. If a patent were secured on a program, it would be unlawful for anyone to make, use, or sell the invention without the authorization of the patentee.[27] Furthermore, by protecting the concept rather than the form in which it is expressed, a broader basis of protection is established.

In a recent case, *In The Matter of The Application of Charles D. Prater and James Wei*, decided November 20, 1968, the United States Court of Customs and Patents Appeals, against the objection of the Patent Office, held that a computer program can be patented. The program in question was a process for measuring the relative proportions of various gases in mixtures using an analog computer. In general, the fight over patentability of computer programs pits the software companies, which generally favor patents, against the hardware manufacturers and a clear concept as to the extent of patentability of programs may not emerge for some time. Even the above decision may not become a governing principle in this area, since the Patent Office's Petition for Rehearing has been granted by the Court, and reargument has been ordered.

A third area of possible protection is contained in the law of trade secrets. This does not involve statutory protection, but is a form of legal protection derived from equity and common law. Through this, an injunction could be obtained against a disclosure or use of a trade secret, and damages and/or an accounting may be awarded. It has been

[24] 35 U.S.C. 101.
[25] 35 U.S.C. 102, 103.
[26] 829 O. G. Pat. Off. 865 (1966).
[27] 35 U.S.C. 271.

stated that service bureaus and other software houses in general regard their programs as trade secrets.[28] The main requirement to secure this protection is simply that the program be kept secret, and this can be achieved by software houses through contracts with their employees. This protection is somewhat limited in that neither the independent creation of an identical program nor the use of similar techniques is prohibited. But it does seem to offer some quantum of protection, easily obtainable, and at minimal cost.

The general problem with protecting the computer program through any of these three methods is that the form which the program takes and the typical use to which it is put do not readily lend themselves to discovery of unauthorized copying or infringement. That is, the program is nothing more than a series of logical steps toward the solution of a problem. In most cases, and especially in more complex problems, these steps can be rearranged to arrive at the same solution. If the program has been pirated, such rearrangement could effectively disguise the program's source. Also, most stolen programs would be used by software houses for their own clients, or by individual users for their own programs, and may never be seen by anyone except the employees of the thief. It would be extremely difficult to police such a system, and locating thievery and tracking down the thieves would be quite expensive. In this respect the law of trade secrets could offer the level of protection needed to provide redress against obvious copying of crucial programs that may cost millions of dollars.[29]

One further consideration is the apparent high level of voluntary cooperation and interaction between organizations involved in formulating programs. There apparently is quite a widespread exchange of data and information within the industry which contributes significantly to its overall growth. To allow full-scale protection may inhibit this interchange and blunt the innovative edge of the industry.[30]

The answer to the outstanding questions of copyrightability and patentability may be forthcoming soon. Legislation has been introduced to revise both the patent and the copyright laws.[31] The Copyright

---

[28]See *Note, Computer Programs*, 81 *Harv. L. Rev.* 1541 at 1554, fn. 126 (1968).

[29]The total cost, hardware and software, of the American Airlines reservation system (Sabre) was $30,000,000. Burck, "On Line in Real Time," *Fortune*, April 1964, at 140, 143.

[30]See generally, *Note, Harv. L. Rev., supra.*

[31]S.597, 90th Cong., 1st Sess., (1967); H.R. 2512, 90th Cong., 1st Sess. (1967) (Copyright Revision Bill); S. 1042, 90th Cong., 1st Sess. (1967); H.R. 5924, 90th Cong., 1st Sess., (1967) (Patent Reform Act).

Revision Bill was passed by the House on April 12, 1967. No action has been taken by the Senate. Section 102 of the Act lays down the requirements of copyrightability in sweeping terms that could encompass computer programs. The protection is extended to "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." Seven categories of "works of authorship" are listed, but none of them includes computer programs. One such category, however, is under the general title of "literary works," which are defined as "works expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects . . . in which they are embodied."[32] The status of computer programs under this general language is not at all clear, but the references to such concepts as "numerical symbols" and reproduction with the aid of "machine or device" suggest at least the strong possibility that computer programs would be copyrightable under the Act. This ambiguity may be resolved before the bill is passed by the Senate, for the Senate has passed a bill, not yet acted on by the House, to establish a Commission to investigate the various problems relating to computers and machine reproduction.[33]

The ambiguity in the Copyright Revision Bill was explained by the House in terms of "the danger of legislating prematurely in this area of exploding technology." Instead of attempting to deal with this problem explicitly, the House Committee felt that "the statute should be general in terms and broad enough to allow for future adjustment to future changes . . ."[34] Although it is difficult to predict the outcome of the Copyright Revision Bill, the Senate bill calling for the establishment of a Commission to study the subject suggests that the revision should possibly deal explicitly with the issue and that substantial changes may be made in the content of the proposed legislation.

The proposed revision of the patent laws is clearer. The Patent Reform Act § 106, provides that programs are not patentable under any circumstances.[35] It seems probable, therefore, that despite the fact that many commentators have called for patent protection, the Patent Reform Act, or one similar to it, will be passed eventually and will not afford protection to computer programs.

---

[32]Copyright Revision Bill § 101.

[33]S. 2216, 90th Cong., 1st Sess., (1967). S. Rep. No. 640, 90th Cong., 1st Sess. 2, 5 (1967).

[34]H. R. 2237, 89th Cong., 2d Sess., pp. 53-54 (1966).

[35]S. 1042, 90th Cong., 1st Sess. (1967); H. R. 5924, 90th Cong., 1st Sess. (1967).

Antitrust Aspects of the Computer Industry

The computer industry can be divided into two basic areas -- hardware and software. The hardware segment includes the manufacture of the machines themselves, their component parts, and related peripheral equipment. The software segment of the industry can be defined as everything other than hardware manufacture. The software itself is nothing more than the program which instructs the computer on its function. But the software industry involves many types of operations. There are four types of services offered by software firms: a) they may simply rent computer capacity, b) they may formulate and rent out generalized proprietary programs, c) they may offer consulting and/or systems analysis services, and d) they may contract out their programming services to a client for a particular job.[36] Thus, there are software houses which specialize in programming services either on a contract basis with a particular user or for their own leased computers. Other firms may prepare "proprietary" programs of general applicability for sale, or programs for hardware manufacturers. There are also service bureaus, which specialize in providing computer facilities as well as programs. Furnishing facilities and programs overlap to a great extent, and with the expansion of the field in recent years, these two activities have actually lost their separate identity as distinct categories in the computer field.

Another activity that can be included under the general rubric of software is that of various information services. This segment is involved in the collection, processing, and sale of information itself. It uses its own information rather than the customer's, and thus it is selling a product distinct from the program. For example, a credit inquiry service would keep in computers records on the credit status of many people and offer to reveal such information for a price. In addition, there are the fringe groups such as corporations which sell computer services as a sideline. Most of this activity is centered in banks which utilize computers in their own operations and take advantage of excess capacity by offering services or leasing time on the machines.

The hardware industry is dominated by IBM which accounts for approximately two-thirds of the output in the hardware sector. There are, however, a number of competitors despite IBM's commanding position. Exhibit 2-B of the *IBM Response in FCC Docket 16979*, Vol. 1, lists the names of new entrants into the hardware field between the

[36] *Justice Department Response in FCC Docket 16979*, p. 9.

years 1949 and 1967. This list contains several dozen manufacturers, including 21 new entrants in the last three years. The equipment capability and performance furnished by the manufacturers also ranges across a broad spectrum of potential commercial and scientific uses. IBM's leading competitors are Control Data Corp., Honeywell, Inc., RCA, Burroughs Corp., GE, Univac Division of Sperry-Rand, NCR, and Scientific Data Systems. The volume of business likewise has escalated in recent years. Scientific Data Systems, Inc., for example, increased its total sales from $1 million in 1962 to $20.4 million in 1964.[37]

The most significant factor in the hardware industry has been the very rapid rate of technological change. Improvements are constantly made, new designs are brought out with increasing rapidity, and the rate of obsolescence is very high. Consequently, barriers to entry into the hardware field should be rather high. A large initial investment would be required, and because of rapid technological change, it probably would not be feasible to attempt to enter the field with a small enterprise. On the other hand, the supply has not kept up with the demand. Consequently, the high risk investment required may result in large dividends if a satisfactory product can be devised and marketed. And in this respect, despite IBM's dominance, many of its competitors while possessing only a small share of the hardware market are giants in the electronic field in their own right, and have the capability to exert pressure on IBM through their research budgets and marketing capabilities.

The first antitrust question that naturally arises involves IBM's dominance of the hardware market. The market nature, however, seems to indicate real competition despite the percentage of IBM's share. It seems, at least right now, too early to make any projection of market shares in the future. The rate of technological change is, as stated above, the key fact of the industry, coloring every part of its operation. This suggests a situation of uncertainty. One hardware company may come up with a distinctly superior product, and could jump to a very large share of the market almost immediately. In this respect, it should be noted that patent licensing by all manufacturers is the rule in the industry, and this would enhance the significance of an important new technological breakthrough. Nevertheless, the Justice Department has brought an action against IBM alleging that it has attempted to monopolize and has monopolized the market for general purpose digital com-

[37]See *Bus. Week*, Mar. 20, 1965, at 172.

puters in violation of Section 2 of the Sherman Act.[38] In addition, three private antitrust suits have been brought against IBM by Control Data Corporation, Data Processing Financial & General Corporation and Applied Data Research, Inc. It is clear that IBM's dominance makes it suspect in everything it does, and it is somewhat restricted in the new fields that it can enter, and new acquisitions that it can make.

Another area of potential antitrust concern is the fact that some hardware manufacturers have moved directly into the software industry. These manufacturers have for several years produced software as well as hardware in addition to the normal incidental services such as systems design and maintenance. Apparently, hardware manufacturers supply assembly and executive programs as a matter of course.[39] Also, some manufacturers offer some proprietary programs of general application and may do some specific contract programming. Their staffs prepare these general programs and distribute them free without regard to the amount of hardware purchased or leased.[40] These programs are given away, but the price, of course, is included in the price of the hardware itself. One critic has suggested that the manufacturer by this method effectively ties his system software to his hardware so he thus has less incentive to develop efficient system software. Software houses, according to this critic, afford no competition to this tying practice of the hardware companies.[41] Because this practice greatly reduces the number of users willing to go to software firms for special adaptation, many software firms help hardware manufacturers develop programs. There seems, however, to be a move away from this practice of free distribution of programs with hardware sales, and the manufacturers' share of the software market is decreasing.[42]

Such arrangements as this free distribution of software hint at "tying" arrangements which may be *per se* illegal under the antitrust laws. Cases finding tying arrangements illegal have concerned agreements by a party to sell one product only on the condition that the buyer purchases a different product: The essence is a single seller tying two separate products together.[43] Here, however, there is no sale

[38] *U.S.* v. *IBM*, complaint filed January 17, 1969, U.S. District Court, S.D. N.Y., C.A. 69 Civ. 200.

[39] See James McKie, *Economic Memorandum*, p. 25, in Vol. I of *IBM Response in FCC Docket 16979*.

[40] See *Note, Computer Programs*, 81 *Harv. L. Rev.* 1541 at 1544 (1968).

[41] Irwin, *The Computer Utility-Competition or Regulation ?*, 76 *Yale L. J.* 1299 (1967).

[42] See *Note, Harv. L. Rev., supra.*

[43] See, *e.g., N. Pac. Ry.* v. *U.S.*, 356 U.S. 1 (1958); *Goodyear Tire and Rubber Co.* v. *FTC*, 381 U.S. 357 (1965).

per se, since the programs are extensively distributed free of charge, and apparently without regard to the amount of hardware purchased. Also, the products are not completely unrelated– in some sense it is natural that the hardware manufacturer would supply some software (especially assembly and executive programs). IBM has announced that it is studying changes in the way it supports its equipment and charges for it and that such changes will be made public no later than June 1, 1969. The joint pricing of hardware, software and related support is one element in the suit filed against IBM by the Justice Department as well as the private suits previously mentioned.

One interesting sidelight to this area is that IBM is presently operating within the terms of the 1956 antitrust consent decree.[11] Under the terms of this decree, IBM was forced to abandon the "service bureau business" directly, and required to establish a subsidiary, Service Bureau Corp., which could not use the name IBM, or employ any IBM employee, or deal with IBM except on a nondiscriminatory basis. The "service bureau business" was defined in the decree to mean preparing with the aid of computers any accounting, statistical, and mathematical information and reports for others on a fee basis. It has been reported that the Justice Department is considering whether to institute action to determine whether IBM's time-sharing services are in violation of this decree. IBM has claimed that it is not acting in violation of the decree, because in time-sharing, the customer processes and handles his own work and is simply afforded access to a computer.[15] Nevertheless, IBM subsequently deemed it expedient to transfer its time-sharing subscriber services to its Service Bureau Corp. subsidiary.[16]

The software area of the industry, composed of quite diverse data processing operations, is highly competitive. The principal requirement for entry seems to be nothing more than the skill of the firm's programmers, and thus it takes relatively little capital to start a venture. The software house may have its own computer, or it may do nothing more than supply programs to the user with the latter leasing or purchasing his own computer. In fact, many of these software houses are started by programmers who formerly worked for hardware manufacturers. A 1966 estimate indicated that there were from 1400-1800 service bureaus in the United States.[17] According to a study made

[11] *U.S.* v. *IBM Corp.*, 1956 CCH Trade Cases, para. 68, 245 (S.D.N.Y., 1956).

[15] *Wall Street Journal*, October 1, 1968.

[16] *Wall Street Journal*, October 23, 1968.

[17] See McKie, *Memorandum*, *supra*, pp. 5-6.

by the Association of Data Processing Organizations, Inc., (Adapso), smaller software firms are growing significantly faster than larger firms. The ten largest firms experienced a growth rate of 19% from 1965 to 1966, while the whole group of firms grew 50% in the same period.[48] In the presence of such wide-open entry and flourishing growth, there seems to be no ground on which to project a future antitrust inquiry into the software segment of the computer industry not connected with hardware manufacturers. The main problem in the industry is the shortage of programmers, a shortage that will probably only grow more acute.[49]

Export Controls on Computers

Computers are subject to certain export controls imposed by the United States Government. The basic statutory scheme is contained in the Export Control Act of 1949, 50 U.S.C. App. 2021-2032. Under this Act the President is given the wide discretion to limit, restrict, or prohibit entirely exports to any person or any nation of any or all commodities. "The requirements of foreign policy, national security, and domestic shortages are the only test."[50] In Executive Order No. 10945, May 24, 1961, the President delegated his power to control exports under the Act to the Secretary of Commerce. Pursuant to this delegation, the Secretary of Commerce has issued a commodity control list, which sets out the export controls applicable to each commodity on the list for each country.

The two basic considerations for export controls are the country of destination and the commodity to be exported. Under the commodity control list requirements, a validated license is necessary to export computers to any country in the world. The potential exporter must make a formal application for a validated license in accordance with procedures set forth in the comprehensive export schedule.

A validated license may be applied for to export computers to any country in the world, including North Viet Nam, Communist China, etc. To the countries in groups XYZ, however, (this includes Hong Kong, Albania and most of the Eastern European countries, Russia, Communist China, North Korea, North Viet Nam, and Cuba) nothing at all sophisticated is allowed to be exported. Moreover, exports to North Viet Nam and possibly a few other countries presumably could be controlled generally under the Trading with the Enemy Act. Two

---

[48] McKie, *Memorandum*, p. 6; *Adapso Study*, p. B-27.

[49] See generally *Note, Harv. L. Rev., supra*, at 1545-7.

[50] S. Rep. No. 1576, in 1962 *U.S. Code, Cong. and Adm. News*, p. 1817.

further points must be noted. First, computers used in defense systems, bearing a military designation, or employed in missiles or space vehicles require special State Department authorization to be exported.[51] Thus, the commodity control list applies only to the garden variety commercial computer. Also, technical data relating to computers and computer operation are governed by regulations issued by the Secretary of Commerce.[52] The export of technical data is defined as any release of unclassified technical data for use outside the U.S. This applies to all data concerning computers. Again in this area, the controls are not strict except that exports of technical data to Communist countries and Hong Kong (XYZ) are closely supervised.

A recent revision of the regulations indicates that the Department of Commerce is showing more concern about exportation of computers. New regulations were issued effective April 1, 1968, which require more detailed information with regard to specifications and capabilities of electronic computer equipment. This is to enable the Export Control Office to make positive identification of the particular commodities to be exported. Para. 373.50, *Comprehensive Export Schedule* requires that an application for a validated license to export computers shall include this specific information. For example, in applying for an export license for analog computers, there shall be disclosed, "(1) the quantity and accuracy rating of each type of summer, integrator, multiplier, or function generator employed; and (2) a description of any capability for the automatic insertion of or alteration of problem setups and of any incorporated device functioning solely as a memory." This revision of the regulation suggests that perhaps closer scrutiny will be given to applications for export of computers, at least to Communist countries. It also suggests that with the technological explosion, and the increasing sophistication of many different varieties of computers, general regulations dealing with computers across the board are not consonant with the proper regulation of exports under the Act.

Certain members of Congress are opposed to the export of any and every commodity to Communist-dominated countries. The computer is no exception. A recent example of this was a concurrent resolution introduced on May 1, 1968, by Congressman Blackburn, Rep.-Ga. This was a "concurrent resolution to express the dissatisfaction of the Congress of the United States with the negotiations to sell, and the subsequent sale of, advanced computer systems and component parts of [sic] Communists nations by certain American business

[51] See para. 370.5, *Comprehensive Export Schedule*, Department of Commerce.

[52] Para. 385.1, *Comprehensive Export Schedule*.

corporations.'"[53] This resolution was referred to the Committee on Interstate and Foreign Commerce and has not been heard from since. The glamour and awe-inspiring complexity of the computer make it a visible target for pressure from certain members of Congress to limit its export.

The response of the Electronic Industries Association to the FCC inquiry in Docket 16979 contains some discussion of the prospects for the foreign computer market. "It is generally predicted that the European market will grow at even a larger rate than the U.S. and that the value of computers of U.S. manufacture installed outside the U.S. should equal in 1977 that installed in the U.S. today."[54] Also, this Association reported that:

> During 1966, U.S. manufacturers exported $296 million worth of electronic computers and parts compared to exports of $223 million during 1965. Preference for the more sophisticated U.S. equipment in foreign markets is evidence of the American technological superiority. Selected equipment from U.S. corporate product lines is being assembled or manufactured in foreign-based sudsidiary plants of U.S. manufacturers or in indigenous plants, as the result of licensing or joint-venture between the United States and foreign corporations. The computing industry's export trade, therefore, reflects only a part of its business in foreign markets. *EIA Response*, p. 13.

According to the 1966 report of the American Federation of Information Processing Society, the foreign computer market is projected to grow by leaps and bounds. In 1965 this foreign market totaled approximately $3 billion. By 1975, the market is expected to reach $8 billion, although the American companies' percentage of this market will not be as large as it presently is because of the expected increasing competition of foreign producers.[55]

It would be hazardous to attempt to make any predictions about the possibility of future controls on the export of computers. Certain conclusions, however, can be drawn with reasonable certainty. First, that aspect of the computer industry dealing with missile guidance systems and other computer uses in the space and defense industries are a special case. These, as stated above, require State Department authorization. It can be expected that such authorization will continue

---

[53] H. Cong. Res. 773, 114 *Cong. Rec.*, H. 3214, May 1, 1968.

[54] *EIA Response*, p. 12.

[55] *EIA Response*, p. 9.

to be required, and that every protection will be afforded to such crucial parts of our national security. Secondly, barring a drastic domestic shortage, computer exports to the non-Communist nations, especially the large European market, will not be subject to more severe control than presently exists. From a technical standpoint, it would seem that the normal commercial uses of a computer—data processing and retrieval—are only tangentially related, if at all, to issues of national defense and security.

It is only in the area of exporting to Communist countries that we may expect to see, at some time in the future, more severe controls. As described above, the present requirement is that a validated license be applied for and received before export can be made. The present practice is to disallow or frown upon exports of more sophisticated devices to Communist countries. Thus, a crackdown could be made through a revision of administrative practice, rather than through changing regulations or the law. Whether more severe controls would be instituted is a function of how important the Commerce Department thinks computers are as a whole in our system of national security. That the Department apparently dislikes exports of more sophisticated devices now could mean that as American computer technology improves and more wondrous devices are constructed, tighter controls may be expected.

Congressional Action in the Computer Field

The development of the computer has heightened concern in many quarters about the problem of protecting privacy in modern society. The computer dramatizes this issue in two related ways. First, its sheer capacity to store, classify, and retrieve immense amounts of data at astonishing speeds means that more and more data now can be collected and used in a meaningful way. Without the capacity offered by a computerized information system, there is a comparatively low limit on the amount of information that can be productively correlated and filed. With the computer, however, the only limit imposed on the value of information is that inherent in the information itself. The second aspect of the computer's impact on information systems is the fact that such data can be centralized to a great extent. For example, many government agencies now collect information from the population for many different purposes and in many different areas. This information is now retained by each agency, but the computer makes it possible to centralize it in one information system.

The issue has been succinctly stated by Professor Westin:

> As we are forced more and more each day to leave documentary fingerprints and footprints behind us, and as these are increasingly put into storage systems capable of computer retrieval, government may acquire a power-through-data position that armies of government investigators could not create in the past eras. Westin, *Privacy and Freedom*, Atheneum, New York (1967), p. 158.

The technological advances in the computer industry have occurred very rapidly, and with the growth of computer systems in general, the problem of privacy protection will probably grow more acute, on the private as well as the government levels. Awareness of this problem has reached as far as the United Nations. In a report of the Commission to Study the Organization of Peace, it was rather dramatically stated that if personal data were integrated and stored on a computer permitting instantaneous access to each person's record, then "a sword of Damocles is going to hang all the time over the head of everybody."[56]

This general problem came to the fore when a series of reports commissioned by the Bureau of the Budget proposed the creation of a National Data Center.[57] The latest proposal was made on the recommendation of the President's Task Force on the Storage of and Access to Government Statistics.[58] The Joint Economic Committee also has recommended establishing such a center.[59] According to Carl Kaysen, Task Force Chairman, the creation of this center will not *per se* result in new information being collected; rather, it involves only centralizing information already in existence. Also, "this system won't have as its aim or purpose to furnish information on individuals. It will have as its aim to furnish statistical information on groups of individuals."[60] The Task Force Report revealed that currently 21 agencies of the federal government have significant statistical programs. The four largest are the Census Bureau, the Bureau of Labor Statistics, the Statistical Reporting Service of the Department of Agriculture, and the Economic Research Service of the Department of Agriculture. Approximately $125,000,000 is spent on this "federal statistical

---

[56] *U.N. and Human Rights*, the 18th Report by the Commission to Study the Organization of Peace, reprinted in 113 *Cong. Rec.*, S. 14518, October 19, 1967.

[57] Ruggles Report, Dunn Report, and Kaysen Report. See "Privacy and the National Data Bank Concept", H. R. No. 1842, 90th Cong., 2d Sess. (1968).

[58] For the Report of the Task Force, see *Computer Privacy*, Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, p. 25, 90th Cong., 1st Sess. (1967). (Hereafter referred to as *Hearings*).

[59] U.S. 90th Congress, "The Coordination and Integration of Government Statistical Programs," Joint Economic Committee, August 1967.

[60] Statement of Carl Kaysen, *Hearings*, p. 15.

system" each year, and each agency collects its own information independently of the others.

Once it is suggested that this information, now spread over various departments, be centralized, the prospect is raised of pushing a button and receiving a personal and revealing file on various aspects of each citizen's life. Such a possibility would obviously be at odds with our basic notions of privacy. According to Dr. Kaysen, it would not be difficult to code the basic information system so that the user and the purpose for which the data is used would be recorded, thus leaving a trail by which the user may be tracked. Or, he suggests, there could be specially coded identifying numbers, which could be encrypted to restrict the category of users. He concludes that it is not difficult to make this system secure against misuse and penetration, for safeguards against illegitimate use of data can definitely be built into such a center. Apart from technical safeguards, the Task Force Report recommends that Congress enact a general statutory standard governing disclosure of information collected on individuals. The director of the proposed federal statistical system would then be given responsibility for monitoring compliance with it. Assuming these statutory standards carried with them penalties for violations, such penalties would hopefully provide some deterrence to the unauthorized use of data. However, the damage in such a sensitive area is done once the data is revealed, and technical safeguards built into the system to prevent revelation in the first instance is by far the most desirable solution; even a necessary solution with personal freedom of such magnitude at stake. Of course, even such safeguards would not prohibit authorized users from having access to the information, and the bureaucratic temptation to make use of readily available information would be extremely strong.

Other witnesses before the subcommittee and the subcommittee chairman himself, Senator Edward Long of Missouri, were not so optimistic about safeguarding the information in such a center. Some witnesses in fact congratulated the subcommittee for their early appreciation of the magnitude of dangers involved in such a center and called either for outright rejection of the proposal to establish the center, or for strict controls and standards to be placed on its use. Professor Arthur Miller of the Michigan Law School pointed out that in the past the privacy of the information collected by the various agencies has depended to a large extent on its very decentralization; i.e., the inability of the snooper to get quick access to large amounts of information. Now, the incentive for gaining unauthorized access to this information is greatly enhanced, since the payoff for snooping is high

in a centralized data center. This suggests that the technical safeguards that Dr. Kaysen says are possible would have to be almost foolproof to withstand the projected all-out attempts to gain access to the information. Professor Miller concluded that the control over the proposed center should be lodged outside existing administrative channels—in a completely independent agency, bureau, or office to be established for that purpose.

In partial rebuttal to Prof. Miller, the Task Force Report points out that at present there is no standard disclosure policy applicable to the various information-collecting agencies. In some agencies there is a formal statutory policy, while in others the policy rests with the whim of the administrator. Enforcement of these varying policies is also quite uneven. Thus "[i]t is quite possible that without some overall policy which can be responsibly supervised major violations of individual privacy may take place."[61]

A year before the Senate hearings took place, a House Subcommittee investigated the same question.[62] The House hearings tended to follow the same lines of testimony as those in the Senate. Incidentally, it was revealed in the House hearings that the proposed data center would cost between $3-3-1/2 million and would take three to five years and 20,000 reels of magnetic tape to stock with the federal statistics now in existence. Paul Baran, computer expert with the Rand Corporation, testified that the same acute danger of privacy abuse was present in the vision of a "computer utility"; an eventual nation-wide network of public and private individual data systems. He suggested that how the government proposed to handle the privacy problem in the National Data Center would provide some sort of precedent for handling privacy problems in the computer utility once it comes into being.

Most of the other testimony before the subcommittees of both the House and the Senate was vague and unenlightening. A few witnesses endorsed the creation of the center, and stated that the possibilities of abuse could be kept at a minimum. Most other witnesses voiced general fears of abuse and repeated familiar platitudes about the sanctity of individual privacy. There has been no legislation introduced to create such a center; it is now in the conceptual stage. The Bureau of the Budget is currently formulating the details of the organization and operation of such a center, and will submit legislation on it, although no date for submission has been indicated.[63]

---

[61] *Report*, p. 7.

[62] *The Computer and Invasion of Privacy*, Hearings before a Subcommittee of the House Committee on Governmental Operations, 89th Cong., 2nd Sess. (1966).

[63] See letter from Raymond T. Bowman, Assistant Director for Statistical Standards,

The House Hearings resulted in a Report by the Committee on Government Operations entitled "Privacy and the National Data Bank Concept." H.R. No. 1842, 90th Cong., 2d Sess. (1968). This Report summarized the results of the Hearings, and while not advising against the creation of such a center, did strongly recommend that "in the design and implementation of such systems the priority of privacy be asserted. While computerized data bases hold great promise, they must contain procedures which can assure the continuation of freedom of thought and action that is such a vital part of the American tradition."[64] And to ensure that this aspect would receive full consideration, the Report called for no work to be done on the proposal until "privacy protection is explored fully and guaranteed to the greatest extent possible to the citizens whose personal records would form its information base."[65] Also, the committee felt that the most adequate solution was the creation of a "separate and distinct supervisory commission."[66]

Much of the information that would be contained in the center is presently protected by law as to confidentiality. For example, all agencies and departments of the government are subject to the penalties contained in 18 U.S.C. 1905, levied for the unauthorized disclosure of confidential statistical data. 12 U.S.C. 9(a) outlines the confidentiality of information gathered in census studies. 47 U.S.C. 605 requires communications common carriers to guard against the unauthorized disclosure of information passing through their communications facilities. Finally, the response of the Justice Department to the FCC inquiry in Docket 16979 points out that section 5 of the FTC Act (15 U.S.C. 45) gives the Federal Trade Commission broad power to obtain relief against unfair and deceptive methods of doing business in interstate commerce. The Justice Department suggests that the Commission could order data processors, software houses, and other programmers to disclose whether or not they have installed generally accepted safeguards to prevent unauthorized disclosure of information. Finally, failure to adopt available safeguards to protect the privacy of information could lead to tort liability on a theory of negligence.

There are four basic stages in the computer process that afford opportunities to establish safeguards for the protection of data from

---

Bureau of Budget, to Jackson E. Betts, U.S. Congressman, October 3, 1967, reprinted in 113 *Cong. Rec.*, H. 13181, October 10, 1967.

[64] *Report*, p. 5.

[65] *Report*, p. 6.

[66] *Report*, p. 8.

unauthorized disclosure. The first is in the hardware; i.e., the machines themselves. Since the computer is such a sophisticated machine, sophisticated protection devices can be built right into it. For example, circuits can be built to protect files and memory. There are hardware "trapping" techniques available which keep an "audit trail" record of the users of the machine.[67] Various encryption devices and even techniques for scrambling can be installed in the system. Secondly, there are sophisticated software techniques available to protect data. For instance, the user may be required to furnish a unique identification code to gain access to the data stored in the machine. There apparently many other variations of this coding method, such as call-back, answer-back, station and personal identification procedures. Another technique is the encryption or coding of the data that is actually stored in the computer. This means that if some unauthorized person should gain access to the computer and retrive the data he would be unable to understand it if he could not decode it. Finally, there is the simple technique of controlling physical access to the computer. The computer terminal could be kept in a locked room with only authorized persons possessing keys. Software houses and government agencies also could be very careful in their selection of employees and maintenance personnel who would have access to the machines.

In short, without exploring the complex technical aspects of the problem, it seems that with these four general categories of safeguards available, definable types of protection can be achieved. Absolute protection in every instance would be, of course, impossible; and the extensive application of safeguards as outlined above would probably be expensive. But the point is that the physical, mechanical, and electronic potentialities exist to provide basic protection for computer-stored information.[68]

There are several general areas of potential federal action in this area. As noted above, statutes already exist which provide some protection to data collected by the federal government. It may be expected that Congress would enact other federal controls over federally-collected data if and when legislation is introduced to create a National Data Center. In the area of private information systems, action by

---

[67] See *Justice Department Response in FCC Docket 16979*, p. 100.

[68] Testimony to the adequacy of various techniques to protect data may be found in the fact that classified military information may eventually be stored in a computer. The MULTICS time-sharing system at MIT is being seriously considered for this use. See *Justice Department Response*, FCC Docket 16979, p. 100, fn. 52.

several agencies is possible. First, the FCC may step in on the communications aspects of computer services—its *Notice of Inquiry* in Docket 16979 suggests that it is sensitive to this aspect of computer services and communications. As suggested in the *Justice Department Response*, the FTC may act to insure that companies will disclose whether or not they have installed encrypting devices and other safeguards for the protection of data. In its response, the Justice Department suggested five other methods of protecting privacy through federal regulation. These are: (1) some system of licensing and inspection, (2) some method of system certification, (3) some method of licensing personnel, (4) compulsory insurance and/or bonding, and (5) criminal sanctions.[69]

Basically, however, the issue of secrecy and protection in the private use of private computers will probably be considered a matter of contract between the user and the computing service. Since techniques are apparently available for protecting computer-stored information, the industry may be expected to formulate a scale of charges varying with the degree of protection desired. In sum, there seems to be no pressing need for federal regulation in the area of private use, especially since there have apparently been no recorded examples of actual abuses and invasions of privacy of this kind; rather, only the specter of such abuses has been raised.

Finally, there is a potential Fifth Amendment problem concerning the disclosure of computer-stored data. In the *Response of Computing and Software Inc.* to the FCC Inquiry, it is stated that "today the computing center which processes information for a client can be forced by court order to supply information which the supplier considers private." (p. 6) The *Response* calls for the creation of a privilege between the user and the computing center similar to the attorney-client privilege with regard to the disclosure of private data. "The fact that an individual chooses to use an outside service agency to process his information should not prejudice his rights under the Fifth Amendment any more than had he chosen to do it internally." *ibid.* Along these same lines, there was a recent amendment to the Delaware Corporation Code which provides for the inspection of corporate computer-stored records and other information not legible visually.[70]

---

[69] *Justice Department Response*, Docket 16979, pp. 95-106,.

[70] This is discussed in an article by Roy Freed in 23 *Business Lawyer*, p. 457, Jan. 1968.

Congressional Concern Over Banks and Computers

The banking industry has gone into the computer service business and certain parts of the latter industry don't like it. There has been pressure in Congress to act against this trend, and bills have been introduced to stop it. H. R. 112, H. R. 177, H. R. 10529 were all introduced in the first session of the 89th Congress to prohibit banks from engaging in certain non-banking services, among them the business of leasing personal property and performing professional accounting and other such services. While these bills as introduced did not specifically include data processing services, this was a relevant issue before the House subcommittee that held hearings on the bills, and certain testimony at the hearings dealt with it.[71]

The present statute, 12 U.S.C. 24(7), indicates that a bank may own and operate data processing equipment. This statute provides that the banks have the power "to exercise. . .all such incidental powers as shall be necessary to carry on the business of banking." The Comptroller of the Currency has indicated that a national bank may purchase majority interest in a data processing company which will provide banking services to it and independent customers. Such an operation was stated to be ". . .clearly incidental to the banking business and this office will interpose no objection . . ."[72]

The banking industry argues for continued allowance of this function on two grounds. (1) Banks, especially larger ones, are required by the exigencies of business to install large computer systems. They thus cannot avoid the problem of excess capacity. Consequently, the argument runs, they might as well use the surplus to serve customers by offering service bureau services. (2) Banks are the only institutions that are spread throughout the country to give smaller users these computer services. Specifically, they are situated in every community of any size across the country and are the only institutions offering these services in many communities.

In his testimony before the House Subcommittee, Herbert Robinson, chairman of the board of C.E.I.R., Inc., and a spokesman for the Association of Data Processing Organizations, Inc., met these arguments this way:[73] The banks don't have to have excess capacity, since they don't need to lease their own computer systems. They can

[71] *Hearings before the Subcommittee on Bank Supervision and Insurance of the Committee on Banking and Currency*, 89th Congress, 2d Sess., March 1966.

[72] Letter from James J. Saxon, Comptroller of the Currency, to unnamed party, March 11, 1966, contained in the 1965-66 *Annual Report, the Comptroller of the Currency*, p. 229.

[73] *Hearings*, p. 121.

rather plug in on a telephone line to a central computer. He hinted in fact that the banks make this argument of excess capacity merely from a desire to move into this extraneous service bureau activity. This same possibility of telephone hookups (part of a larger vision of a "computer utility") also cuts some of the ground from under the banks' argument that they offer computer services to people who cannot get them anywhere else. Mr. Robinson further cited the growth and spread across the county of data processing businesses, so that there are computer services offered in most every community that computer-equipped banks reach. Mr. Robinson also vehemently attacked the competitive advantages enjoyed by large banks by virtue of their "unique quasi-monopolistic position." He expressed the fear that with the banks' great financial resources, their prestigious position, their advertising and sales promotion coverage, and their clients' obligations to them, they would snuff out small service bureaus if they entered the data processing industry on a full scale. He thus pressed for an amendment to the bill that would add the words "data processing services" to the list of prohibitions to be enacted against banks.

As it turned out, this bill apparently died in committee. However, the experience does point out the far-reaching implications of the computer industry across a wide field of economic activity. It also illustrates the speed with which proposals for handling the growth of this industry will at least reach Congress, if not be enacted into law.

The Government As A Consumer of Computer Services

While not an aspect of federal regulation of the computer industry, the application of computers in the performance of various governmental functions may throw some light on the general problem of federal regulation of computers. This topic has been the subject of exhaustive hearings in Congress, and resulted in 1965 in the enactment of a law attempting to standardize and regulate the government's purchase, lease and employment of computers. This law, amending Title 1 of the Federal Propery and Administrative Act of 1949, demonstrates the government's awareness of the overall value of computers and indicates the need for a coherent comprehensive policy in government computer use.

A few statistics can provide some background.[74] The federal government is the largest user of automatic data processing in the world. At the time the cited Senate report was written in October 1965, the government annually expended $3 billion on computer systems.

[74]These are taken from S.R. 938, 1965 *U.S. Code, Cong. and Adm. News*, p. 3860.

Again at that time, automatic data processing usage in the government was doubling every three years. The first all-electronic computer was put into operation in the Army Ordnance Corps at the end of World War II, in 1945. Univac I, the first computer with general data processing capability, was first used by the Bureau of the Census in 1951. In 1954, there were 10 computer systems in operation. As of 1965 there were 2,000, this number *not* including 1,000-2,000 computers that contractors have purchased or leased at governmental expense. Nor does it include computers used in defense weapons and systems, or in missile and space vehicles. In an address before the American Management Association, Senator Sam Ervin updated these figures for 1966 to include 2,600 computers, with 71,000 federal employees operating these systems.[75]

The substance of the 1965 law, found at 40 U.S.C. 759, has three basic objectives: (1) To provide more adequate management information, (2) to provide optimum realization through sharing and multiple use, and (3) to insure economic acquisition. The latter includes consideration of volume acquisition, lease as compared to purchase, and purchasing the most advantageous equipment on a government-wide basis.

The law applies across the entire range of government involvement with the computer; i.e., procurement, maintenance, operation, and utilization. The General Services Administrator is authorized to coordinate and provide for the purchase, lease, and maintenance of equipment by federal agencies. Also, the Secretary of Commerce is authorized to provide scientific and technological advisory services and recommendations to the President to establish uniform federal automatic data processing standards.

With the government being the largest consumer of computers and computer services, it may be expected that it will acquire first-hand knowledge of the various legal, social, and regulatory problems involved. This is not to suggest that the government acts as a monolithic whole, with perfect communication and feedback throughout the many departments and agencies; the real situation does not, of course, approach this. Nevertheless, the various organs of the government will not be unfamiliar with the computer, and the greater the exposure to its capabilities, the greater the sensitivity to the issues it raises.

---

[75] Reprinted in 113 *Cong. Rec.*, S. 3369, March 8, 1967.